AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

STATE OF WEST VIRGINIA

COUNTY OF MERCER, to-wit:

I, Gary Hilton, being duly sworn under oath, do hereby depose and state:

1. I am employed as a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and am currently assigned to the Charleston, West Virginia Office. I have been employed as a Special Agent since August 2004. I am a graduate of the Criminal Investigators Training Program and ICE Special Agent Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have previous law enforcement experience as a Deputy Sheriff with the Sarasota County Sheriff's Office in Florida, where I was employed from March 1996 to August 2004.

2. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have investigated persons suspected of criminal activity relating to child exploitation and child pornography, including activity pertaining to the illegal production, distribution, receipt and possession of child pornography in violation of 18 United States Code Sections 2251, 2252 and 2252A.

3. This affidavit is being submitted in support of an application for a search warrant for Route 5, Box 382, Bluefield,

West Virginia, also known as 382 French Street, Bluefield, West Virginia 24701, ("SUBJECT PREMISES") which is described in detail in Attachment A. As will be shown below, a person accessing a website located at URL http://www.liberalmorality.com received and/or transmitted via the Internet, images depicting minors engaging in sexually explicit conduct, and that there is probable cause to believe the person who accessed the site is in possession and received and/or transmitted the aforementioned material using a computer that is located at the Subject Premises.

4. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of a violation of 18 U.S.C. §§ 2252 and 2252A is located at the Subject Premises.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252 and 2252A, which make it a crime to receive, possess, and/or distribute child pornography.

RELEVANT STATUTES

6. This investigation concerns alleged violations of 18 U.S.C. Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. Title 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

8. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

9. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

10. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

11. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

12. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

13. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable

television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

14. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov

identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

15. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

16. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

17. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

18. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is

accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

19. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND REGARDING SEIZURE OF COMPUTERS

20. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

21. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

22. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific

procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

23. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored

devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

24. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law, and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

BACKGROUND REGARDING THE INTERNET/COMPUTERS AND CHILD PORNOGRAPHY

25. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since approximately 1995. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

26. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user

accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

27. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a

scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and distribute it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

28. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation.

It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

29. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

30. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside

in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

BACKGROUND OF INVESTIGATION

31. On or about March 19, 2010, the Child Exploitation Section of the ICE Cyber Crimes Center (ICE/C3/CES) received information from the National Centre for Combating Pedophilia Online (Centro Nazionale per il Contrasto alla Pedopornografia On-line or C.N.C.P.O.) located within the Italian State Police Postal and Communication Service that identified a website offering access to child pornographic images and/or video files. The website was identified by the domain name "http://www.liberalmorality.com."

C.N.C.P.O. provided ICE/C3/CES with the corresponding URL: http://www.liberalmorality.com.

32. On March 19, 2010, an ICE agent stationed at ICE/C3/CES, located in Fairfax, Virginia, accessed the provided URL for the "http://www.liberalmorality.com" website. The following text appeared on this website's homepage:

Liberal Morality

Hot Girls

PornStars

Celebrity

Facebook

Suggestions

33. While the words "Hot Girls," "Pornstars," "Celebrity," "Facebook" and "Suggestions" are all intended to be hyperlinks to other locations within the website, only the words "Hot Girls," "Pornstars" and "Suggestions" contained live hyperlinks. The other links were inactive and thus essentially just contained the titled text.

34. When the ICE agent accessed the "Hot Girls" hyperlink on the homepage, he was redirected to a second web page within the website. This web page contained an area which allowed visitors to enter their name, a link (a hyperlink to another location within the internet where a photo might be posted to a different server), a subject (enabling the visitor to enter a subject they choose),

and any comments they wished to add. Additionally, this webpage allowed users to attach a file and password in order to post their own images. This second webpage contained 10 images. Nine of the ten images depicted what appear to be minor females, nude or near nude, and in some of the photos the minor children were naked with their genitals exposed. Another image on this page appeared to be a prepubescent male being anally penetrated by another male. Each photo has what appears to be a file number embedded into the image. The user name "Hello Friends" was also embedded into many of the photographs listed on this page, including the image depicting the prepubescent male described above. The posting date of each photograph was listed along with a hyperlink which in most cases took ICE Agents to a different website entitled "FreeForum.tw," which appeared to be an Asian based webpage. Each photo had a "Reply" section which allowed its viewers to leave a comment about each photo. This page also had links to 34 additional webpages within the website.

35. Many of the images contained within these 34 pages are child pornography, based on the definitions described above. For example, on page 4, a digital image with the file name 1268998933266.jpg was posted on March 19, 2010, by an Anonymous poster. File 1268998933266.jpg depicted a young male who appears to be under 14 years of age performing oral sex on an adult male. On page 6, a digital image with the file name 1269016393567.jpg was

posted on March 19, 2010, by an Anonymous poster. File 1269016393567.jpg depicted two young females with long brown hair who appear to be under 12 years of age performing oral sex on an adult male. On page 11, a digital image with the file name 1269012583203.jpg was posted on March 19, 2010 by a user with the screen name "Hello Friends." File 1269012583203.jpg depicted a young nude prepubescent male who appears to be under 10 years of age sitting on a couch with his legs spread and someone is digitally penetrating his rectum. On page 12, a digital image with the file name 1269009922271.jpg was posted on March 19, 2010 by an anonymous poster. File 1269009922271.jpg depicted a young nude prepubescent female who appears to be under 12 years old tied up with black rope with her legs tied and spread apart exposing her genitals and her arms tied together above her head wearing a black eye mask. On page 15, a digital image with the file name 1269003652340.jpg was posted on March 19, 2010 by an Anonymous poster. File 1269003652340.jpg depicted a young nude female who appears to be under two years of age lying down while another young child who appears to be a toddler pulls her labia.

36. When the ICE agent accessed the "Pornstars" hyperlink on the homepage he was redirected to a second web page within the website. Again, this web page contained an area which would allow its visitors to enter their name, any links they wished to include, a subject matter, and comments. They also had the ability to

attach a file and password in order to post their own images. This page contained 12 images. The majority of the images depicted children involved in sexually explicit conduct. Another one of the photos was of a web camera and when ICE Agents examined this post, a hyperlink took him to another page "www.lix.in". This link had the text "Web cams live shows little girls. Nude and NN". On page 0, a digital image with the file name 1269018501201.jpg was posted on March 19, 2010, by Anonymous poster. File 1269018501201.jpg depicted a young nude prepubescent Asian girl who appears to be under 10 years of age lying on a bed with white sheets and is being vaginally penetrated by an adult male. On page 0, a digital image with the file name 1268979696404.jpg was posted on March 19, 2010, by Anonymous poster. File 1268979696404.jpg depicted a young nude prepubescent boy who appears to be under 14 years of age lying on a bed while an adult female with blond hair performs oral sex on him. Unlike the "Hot Girls" link page where it appeared that "Hello Friends" did the majority of the posting, the "Pornstars" page did not have many user names associated with the photos. In the area where a poster's name would appear, it stated anonymous. This page also had links to pages 1 and 2 which were similar in nature to page 0.

IDENTIFICATION OF THOSE WHO ACCESSED THE WEBSITE

37. On the same date that the http://www.liberalmorality.com website was accessed by the ICE agent, an ICE agent accessed a

publicly available service on the Internet, which was used to determine the registrant/owner of the domain name http://www.liberalmorality.com. This service is a free database service capable of identifying, among other things, the owner of a particular domain name and the IP address where the website is located. This database search indicated that the IP address associated with the above listed domain name was 74.208.83.116, and that it was owned by One & One Internet Inc., located at 701 Lee Road, Suite 300, Chesterbrook, Pennsylvania 19087.

38. On or about April 20, 2010, an ICE agent obtained and executed a federal search warrant for the website located at URL http://www.liberalmorality.com. ICE C3/CES reviewed the evidence received as a result of this search warrant. The evidence obtained from http://www.liberalmorality.com, included, among other things, web access logs and the entire content of the website. The web access logs track activity on the website and record all requests processed by the server that contains the website, including downloads and uploads to the server. Each image on the website was displayed as a thumbnail version and a user could obtain an enlarged version of the image by clicking on the thumbnail version. The following provides an example of a image posting on the website: [File: File Name.jpg -(File Size) Thumbnail displayed, click images for full size.]. The web access logs include any "get" commands, which are generated when a user's web browser

requests/accesses a file from the website. The logs indicate which version- thumbnail or enlarged- was accessed. The typical format for a web access log is: [IP ADDRESS] [TIME/DATE STAMP] [REQUEST - "GET" OR "POST" COMMANDS]. The following provides a sample of a web access log extracted from the evidence obtained from http://www.liberalmorality.com 76.122.237.14 18/Mar/2010:23:35:03-0400] "Get /ps/src/1268957091316.jpg. In this example, the IP address 76.122.237.14 accessed the image file 1268957091316.jpg on March 18, 2010 at 23:35:03.

39. The evidence obtained from http://www.liberalmorality.com contained web access logs from approximately March 15, 2010 through March 19, 2010. The web access logs were all similar in structure as the example provided in paragraph 40. ICE C3/CES was able to extract the specific files from http://www.liberalmorality.com that were identified in the web access logs and, therefore, match IP addresses with specific image files that were accessed from each IP address. Administrative subpoenas were sent to the appropriate ISP's to identify the subscriber assigned that IP address on the date and time it was used to access child pornography image files on the http://www.liberalmorality.com website.

THE SUBJECT OF THIS SEARCH WARRANT

40. As stated above, ICE C3/CES executed a federal search warrant for the website located at URL http://www.liberalmorality.com and was able to identify IP

addresses used to access specific image files on the site. The subject of this search warrant was assigned an IP address at the time it was used to access child pornographic content on the http://www.liberalmorality.com website.

41. The web access logs from this website indicate when a user accessed the website and the specific files the user accessed and received, or attempted to receive. A review of the web access logs for the IP address assigned to MOODY at the relevant time revealed that the user accessed the website and obtained numerous visual depictions of minors engaged in sexually explicit conduct including enlarged (full size) images of child pornography. Enlarged (full size) images of child pornography are obtained from the http://www.liberalmorality.com website by a user clicking on the thumbnail image. The thumbnail images, as displayed, were of sufficient size for a user to identify the nature and content of the images. For example, according to web access logs from the http://www.liberalmorality.com website, the IP address assigned to MOODY on March 19, 2010, beginning at 03:18 was used to access child pornography. The web access logs from this website indicate when a specific customer accessed the website and the specific files he/she accessed and received or attempted to receive. A review of the web access logs for the IP address assigned to MOODY at the relevant time revealed that the user accessed the member

restricted website and obtained numerous visual depictions of minors engaged in sexually explicit conduct.

The following provide three examples of files the IP address assigned to MOODY accessed and received or attempted to receive:

a) 76.122.237.14
19/Mar/2010:03:25.44 -0400
1268979696404s.jpg

Image 12689796404s.jpg depicts a nude prepubescent male with a white hat lying on his back. An adult female nude above the waist was on the nude prepubescent male's left side leaning over him with the nude prepubescent male's penis in her mouth and holding the penis with her left hand.

b) 76.122.237.14
19/Mar/2010:03:18:52 -0400
1268975445584s.jpg

Image 1268975445584s.jpg depicts a prepubescent female wearing a white t-shirt and pink shorts standing on the left side of an adult male. The adult male was nude from the waist up and had a blue pair of pants pulled down exposing his penis. The prepubescent female was holding the adult male's penis with her right hand as the adult male urinated into a toilet.

c) 76.122.237.14
19/Mar/2010:03:18:52 -0400
1268979621005s.jpg

Image 1268979621005s.jpg depicts a nude minor sitting with a nude adult female sitting on his lap facing away from nude minor male. The nude minor male has his left arm around the waist of the nude adult female and is leaning around with the nude adult female's nipple in the nude minor male's mouth. The nude adult female's legs are spread apart and the nude minor male's penis is inserted into the nude adult female's vagina.

42. On or about August 6, 2010, ICE C3/CES issued an administrative subpoena to Comcast Cable Communications, for information regarding IP address 76.122.237.14 from the dates and times contained in the access logs. On or about August 16, 2010, Comcast Cable Communications revealed that IP address 76.122.237.14 was assigned to Rosa MOODY, Route 5, Box 382, Bluefield, West Virginia, and was assigned account number 0173010873902.

43. On or about March 15, 2011, ICE HSI Agents issued a Summons to Comcast Cable Communications for subscriber information associated with Rosa MOODY or provided at Route 5, Box 382, Bluefield, West Virginia. On or about March 22, 2011, Comcast Cable Communications provided information that the subscriber for the residential high speed internet service for Route 5, Box 382,

Bluefield, West Virginia was Rosa MOODY and her account number was 0173010873902.

44. A check with the West Virginia Division of Motor Vehicles on or about March 4, 2011, revealed that an individual named Rosa MOODY with a date of birth of 10/1/1966 resided at the Subject Premises.

45. On or about March 9, 2011, representatives of the United States Postal Service informed ICE agents that Rosa MOODY was at that time receiving mail at the Subject Premises.

46. On or about March 23, 2011, representatives of American Electric Power informed your affiant that service was being provided to Rosa MOODY at the Subject Premises.

47. Surveillance of the Subject Premises on or about March 17, 2011, revealed that the residence was a single-level frame structure with white siding. Brown and white shutters were located on the structure and the roof appeared to be constructed of brown shingles. There was a small porch on the front of the premises. A Ford F-150 truck with West Virginia License Plate 8J6754 was parked in the driveway of the Subject Premises. A search of West Virginia Division of Motor Vehicles records showed that West Virginia license plate 8J6754 was assigned to a 1997 Ford F-150 truck, which was registered in the name of Timothy J. MOODY and Rosa L. MOODY, Route 5, Box 382, Bluefield, West Virginia.

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN RECEIVING CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

48. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and receive multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a) Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b) Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for

their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c) Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d) Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the

individual to view the collection, which is valued highly.

e) Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f) Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

CONCLUSION

49. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the Subject Premises described in Attachment A, in violation of 18 U.S.C. Sections 2252 and 2252A.

50. You affiant, therefore, respectfully subscribes that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Further, your affiant sayeth not.

GARY HILTON
Special ~~Agent~~
Immigration & Customs Enforcement

Sworn and subscribed before me this 14th day of July, 2011

HONORABLE R. CLARKE VANDERVORT
United States Magistrate Judge